Approved on March 31, 2016
Responsible Editor: Raymundo Juliano Feitosa
Associate Editor: Fernando Galindo Ayuda
Evaluation Process: Double Blind Review pelo SEER/OJS

"BIG DATA BIG PROBLEMA! PARADOXO ENTRE O DIREITO À PRIVACIDADE E O CRESCIMENTO SUSTENTÁVEL.

[1]Adalberto Simão Filho
[2]Germano André Doederlein Schwartz

RESUMO

Constatado o paradoxo existente entre sistema de proteção da vida privada e da base de dados pessoais quando em confronto com a prática de utilização de dados maciços estruturados e não estruturados que trafegam por internet, por meio de super processadores, denominados de Big Data, a intenção é instigar o pensamento critico construtivo, na busca de proposições que possam harmonizar interesses pessoais de usuários e interesses de outras matizes, na construção do modelo econômico denominado Internet das Coisas- IdC, prestigiando o direito constitucional à vida privada.

Palavras-chave: Big data, Privacidade, Proteção de dados, Vigilância, Autodeterminação

" BIG DATA " BIG PROBLEMA! LA PARADOJA ENTRE EL DERECHO A LA PRIVACIDAD Y EL CRECIMIENTO SOSTENIBLE

RESUMEN

Encontrada la paradoja existente entre sistema de protección de la privacidad y de bases de datos personales cuando se enfrentan a la práctica de utilizar los datos masivos y no estructurados o estructurados que viajan a través de Internet con " Big Data " , la intención és instigar el pensamiento constructivo fundamental en la búsqueda de propuestas que se pueden armonizar los intereses personales de los usuarios y los intereses de otros matices , la construcción del modelo económico llamado Internet de las cosas - IdC , honrando el derecho constitucional a la vida privada.

Palabras-claves: Big datos, Privacidad, Protección de datos, Autodeterminación, Vigilância-

[1] Pós-Doutor Pela Universidade de Coimbra - UC (Portugal). Professor pela Universidade Federal de Goiás - UFG, Goiás (Brasil). E-mail: adalbertosimao@uol.com.br

[2] Pós-Doutorado pela University of Reading – UR (Inglaterra). Diretor Executivo Acadêmico do Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas - FMU, São Paulo (Brasil). E-mail: germano.schwartz@globo.com

Introdução

A sociedade da informação como ambiente posterior à pós modernidade, cuja característica maior é exatamente o expressivo impactos da tecnologia tanto nas relações humanas como nas relações empresariais, sociais e governamentais, apresenta ao estudioso de ciências sociais, desafios concernentes à forma de estruturação por meio digital desta relações, onde todo e qualquer elemento escrito, sonoro, visual, imagens ou mídias de qualquer natureza, se convergem e se transformam em dados que trafegam na velocidade do pensamento, por meio da auto estrada informacional.

O acesso à internet como um dos elementos essenciais ao exercício da cidadania, juntamente com a liberdade de expressão e o direito à privacidade, com clara contribuição para o desenvolvimento da personalidade, formam a disciplina do uso da internet no Brasil onde, ainda, no âmbito do respeito aos direitos humanos, pluralidade e diversidade, se reconhece tanto a escala mundial da rede, no tocante a abrangência de suas complexas relações e ramificações, como também o prestigio ao princípio da livre iniciativa e da livre concorrência.

A Problematização relacionada à privacidade trazida neste artigo, refere-se basicamente ao tráfego de dados e a estrutura cosmopolita da internet mundial. Se, por um lado há o direito pessoal de inviolabilidade da intimidade, vida privada, sigilo no fluxo de comunicações pela internet ou comunicações privadas armazenadas e a liberdade de expressão como condição básica para o pleno exercício do direito de acesso à internet, a outro, criou-se por meio de procedimentos de Big Data, um sistema intenso de processamento de informações que trafegam em internet (dados sensíveis, públicos, sigilosos ou de qualquer outra natureza) possibilitado por softwares e equipamentos que trabalham com um volume maciço destes dados e que são utilizados em áreas das mais diversas, algumas das quais sequer claramente definidas, gerando um mundo onde a característica maior é a formação de valor ao dado coletado; a vigilância constante e o desprestígio à privacidade.

O Artigo pretende verificar se há possibilidade de harmonização dos interesses pessoais e econômicos gerados pelo sistema Big Data, buscando elementos seguros tanto na legislação brasileira como no ordenamento europeu para o desenvolvimento de um sistema eficiente e protetivo da privacidade que não afaste a necessidade de crescimento sustentável e inclusivo.

A vigilância liquida exercida contra todos, por meio tecnológico aliada a necessidade de se gerar efetiva proteção e segurança aos dados e pessoas em ambiente de internet, são os temas nucleares deste artigo. Ao se procurar entender as razões da insistente vigilância e localizar os atores que trabalham com o processamento e monetização de dados maciços, talvez se consiga dimensionar os objetivos consistentes da busca de elementos que possam gerar maior proteção ao usuário de internet, no ponto de sua vida privada.

O tema atual e instigante justifica-se em aprofundamento, na medida em que a cada período, mais países periféricos ingressam em sociedade da informação, fazendo uso da internet em governo eletrônico e nas relações econômicas e sociais. A metodologia de pesquisa parte da análise empírica da observação da estrutura de internet e de seus reflexos decorrentes do tráfego maciço de dados, alem da revisão da literatura e doutrina. O Referencial teórico abrange tanto a literatura atual brasileira e espanhola sobre o tema como autores mundialmente relacionados na sociologia e no direito como Zigmunt Bauman, Manuel Castells, Jeremy Rifkin, Stefano Rodotá entre outros.

1.**Os dados como nova fonte de riqueza e de poder.**

Toda e qualquer informação numérica, alfabética, gráfica, fotográfica, acústica, midiática ou de qualquer outra espécie que sofre tratamento tecnológico com vistas a possibilitar tráfego em auto estrada de informação, é considerada genericamente como dado.

A informação devidamente agrupada com algum critério, conformaria uma base de dados. Mas, como envolve um caráter multidisciplinar (MIRETE-2014), há que se procurar melhor dimensioná-la e entende-la para que se possa estabelecer um regime jurídico protetivo apropriado e eficiente.

Uma base de dados pode ser formada a partir da seleção prévia, inserção de conteúdos, elementos e informações relacionados a uma quantidade de bens de diversas naturezas e organização estrutural racional e eficiente, buscando em seu contorno atender a uma finalidade ou conjunto de finalidades específicas relacionadas a sua utilização.

E é exatamente a forma de estruturação da base de dados de maneira que a mesma possa ser eficientemente pesquisada e esta potencialidade de multiutilização para fins diversos como o econômicos, que acaba por gerar um valor que não se coaduna em muitos casos, com a necessidade de proteção da privacidade do cidadão.

Há dados genericamente considerados e dados de caráter pessoal que devem ser considerados no estudo dos bancos ou das bases de dados e sua função econômica.

O objeto da relação jurídica protetiva no que tange ao tratamento de dados, refere-se aos dados de caráter pessoal.

Partindo da visão Europeia, em especial a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1.995, relativa a proteção das pessoas físicas no que concerne ao tratamento de dados pessoais e da livre circulação destes e a LOPD - Lei Orgânica de Proteção de Dados Pessoais, estabeleceu-se como dado pessoal, qualquer informação numérica, alfabética,gráfica, fotográfica, acústica ou de qualquer outro tipo, concernente à pessoa física identificada ou identificável (GIMÉNEZ et MARTÍNEZ, 2010,p.35).

Estas informações podem ser objetivas e pessoais, como também subjetivas. A proteção destes dados não se refere à veracidade destas informações, mas à qualidade de seu conteúdo pessoal compreendendo desde informações relacionadas à vida privada como também informações sobre qualquer atividade desenvolvida pela pessoa nas suas relações profissionais, econômicas sociais, entre outras.

Há critérios para se considerar uma pessoa física identificada. Esta pode ser considerada como tal quando dentro de um grupo de pessoas, é distinguida dos demais membros deste grupo. A pessoa física é assim identificada quando ainda que não se tenha feito a identificação efetiva, é possível fazê-la através dos dados identificadores disponíveis (SALOM,2013,p.109).

São considerados como dados públicos os dados pessoais que são conhecidos por um elevado número de pessoas sem que o titular possa saber a fonte nem possa impedir a sua difusão, sendo a consciência social favorável a sua difusão. São dados privados aqueles dados pessoais que são cedidos com o consentimento de seu titular, sendo a consciência social favorável a sua privacidade.

No âmbito dos dados pessoais, há os dados considerados sensíveis consistentes de um conjunto de informações pessoais que são particularmente propensas a causar discriminação ou estigmatização ao seu titular, quando forem objeto de tratamento sem autorização, tais como informações que revelem a origem racial ou étnica do titular, as suas convicções religiosas, filosóficas ou morais.

O principio da monetização de dados, não considera se estes são provenientes de bancos de dados generalistas ou se são dados pessoais e sensíveis. O objetivo maior daqueles que se especializam da prospecção de dados com vistas à formação de valor econômico é exatamente a transformação e o enriquecimento da capacidade de monetização destes dados, voltando a empacotá-los de forma tal que os mesmos possam se consolidar em um ativo imaterial que atenda às soluções idealizadas pelo cliente para o uso do meio digital específico (SCHMARZO-2013,p.111).

Os dados e a sua forma inteligente de transformação, utilização e monetização, acabam por formar por si só um aviamento, uma fonte de riqueza e de poder sem precedente do ponto de vista daquele que possa deter a informação atual, clara, verdadeira e selecionada.

Uma base eletrônica de dados se constitui um elemento imaterial que gera ao titular o direito de propriedade intelectual que acaba por resultar ganhos sobre a exploração financeira da mesma. A exemplo do que ocorre com o direito do autor cuja proteção se dá independente de registro, a proteção da base digital consistente de um banco de dados, prescinde de registro para a sua condição de validade (MIRETE,2014,p.157).

A outro lado, o direito sobre uma base de dados, em razão do caráter heterogêneo dos produtos sobre o qual se aplica, aliado à amplitude do conceito de base de dados e especialidade do objeto protegido por este direito, levou na Espanha à consideração de que se trata de um direito *sui generis*.

Esta intelecção encontra-se presente também na diretiva europeia que trata de base de dados. A tutela protetiva se dá em face das extrações e reutilização não autorizada de conteúdos de base de dados. O objeto de proteção deste direito *sui generis* se dá em razão da inversão substancial de capital e esforços realizada pelo fabricante para a criação e a elaboração da base de dados (ALEJANDRE,2014,p.265).

Neste mesmo sentido o parágrafo 1º do art.133.3 do LPI- Real Decreto legislativo 1/1996, prevê: "O direito *sui generis* sobre uma base de dados protege os investimentos substanciais, avaliados qualitativa ou quantitativamente, que realizou o fabricante, seja por meios financeiros ou por emprego de tempo, esforços, energia ou outros de similar natureza, para a obtenção, verificação e apresentação de seu conteúdo".

Forma-se assim um ativo imaterial consistente da base digital de dados cujo direito de operação foi cedido, compartilhado ou transferido para alguém, que pode compor entre outras funções, um estabelecimento empresarial como bem incorpóreo, contribuindo para a sua valoração a depender da qualidade e possibilidade de monetização ou de aviamento deste ativo ou para a realização de negócios jurídicos que possam ser pertinentes com a sua natureza.

2.**A utilização maciça de base de dados - Big Data e as revoluções tecnológicas.**

O termo "*Big Data"* descreve não só uma tecnologia apropriada de captura de dados, como também o crescimento, a disponibilidade e o uso exponencial de informações estruturadas e não estruturadas que caminham pela internet no âmbito da liberdade de expressão.

Informações que resultam em dados estruturados são aquelas objetivamente coletadas e dirigidas, passando a formar um banco de dados específicos. Por sua vez, o conjunto de informações truncadas ou não, que compõem um conceito de dados não estruturados, decorrem tanto da captação autorizada ou não (por meio de cookies ou outra forma tecnológica), dos rastros digitais deixados pelo usuário em internet, quando este trafega em páginas e sites ou, ainda, por sistema de telefonia ou qualquer outro meio eletrônico de comunicação.

Os dados não estruturados são também processados maciçamente por computadores potentes que efetuam cruzamentos de conteúdos e pessoas e análises.

As informações geradas em ligações telefônicas, call centers, troca de e-mails, endereços de busca na internet, uso de caixas e equipamentos eletrônicos, qualidade de postagens em redes sociais ou interesses demonstrados em compras de qualquer natureza, são assim captadas, armazenadas e processadas para compor ou completar um banco de dados específico (SIMÃO FILHO, 2015,p.33).

O resultado prático se faz no sentido de que, com um Big Data em ação, decompondo sistematicamente os dados estruturados e não estruturados, torna-se possível desenvolver negócios dos mais diversos como demonstrado, monetizando o banco de dados, como também operar preditivamente prevendo comportamentos, identificando padrões e descobrindo o porquê de muitas coisas alem de incentivar o consumo e criar políticas internas empresariais para otimizar resultados e auxiliar na tomada de decisão relacionada, entre outros assuntos, ao enfrentamento de crises econômicas, mercados concorrentes ou geração de nova demanda.

O sistema Big Data possibilita o cruzamento de dados numa velocidade e precisão espantosa, cujas consequências são inúmeras em seus resultados como, a exemplo, contribuir para localização de hábitos de consumo, conhecimento de grupos de pessoas propensas a sofrer moléstias custosas, detecção de Jovens com maior probabilidade de incidir em crimes, verificação de hábitos religiosos e localização de pessoas por geolocalizadores.

A propósito, geolocalizadores são ferramentas informáticas que possuem a aptidão de com o uso de coordenadas geográficas, possibilitar a localização física dos usuários ou de equipamentos. A análise de dados maciços colhidos a partir de informações prestadas pelos geolocalizadores, alguns contidos em equipamentos celulares, pode trazer não só a direção IP dos terminais de acesso como também, captar a movimentação do usuário.

O uso desta ferramenta em políticas de geomarketing é intenso e hostil a ponto de acabar por dirigir o usuário a certa linha de consumo ou estabelecimento, pelo simples fato de se ter acesso prévio ao local onde o mesmo se encontra. O usuário não percebe que está sendo influenciado na sua tomada de decisão quando verifica publicidades que se relacionam a produtos ou serviços ao seu redor (JIMÉNEZ et DITTMAR,2013,p.528).

A análise de dados maciços, todavia, não pode ser taxada como algo negativo ou depreciativo, pois, pode gerar também uma série de resultados sociais positivos como esclarecem as pesquisas de Victor Mayer-Schönberger e Kenneth Cukier no âmbito da saúde pública.

Concluíram estes autores que o cruzamento de dados pode se prestar a inibir o crescimento de vírus, a partir da observação na navegação de pessoas, quando estas pesquisam em sites de buscas informações de sintomas, registrando nos argumentos de buscas o que estão sentindo. A análise destes padrões de dados pode contribuir para detectar onde se encontram estas pessoas e exercitar uma política pública de prevenção ou contenção (MAYER-SCHÖNBERGER ET CUKIER,2013,p,09).

O ambiente de sociedade da informação atual gerou basicamente, pelo menos duas revoluções tecnológicas claramente verificadas:

i) **Revolução dos negócios baseados em dados**.Novas fontes de dados gerados por meios sociais e pelo crescimento da telefonia móvel e sistemas digitais diversificados de captação da informação e imagens, possuem potencial de modificar por completo o processo tradicional de geração de valor de uma companhia. A boa aglutinação destes dados, em uma base digital adequada, pode gerar conhecimentos adicionais sobre o interesse, as paixões as afiliações, redes e relações do usuário, alem de elementos de fidelização de tal ordem que se otimize ao infinito o processo de captação e prospecção de clientela(SCHMARZO-2013,p.79).

ii) **Revolução decorrente de implantação da Internet das Coisas - IdC**.Rifikin é o maior defensor desta visão e esclarece que toda a atividade econômica é baseada no aproveitamento de energia disponível na natureza em suas formas, liquida, sólida ou gasosa, que se convertem no processo produtivo em produtos ou serviços. Da utilização da internet em todas as coisas IdC, emerge uma plataforma tecnológica nova e poderosa o suficiente para acelerar o final do capitalismo na forma conhecida e gerar uma contradição paradoxal.Esta plataforma de base tecnológica é fruto da união da internet das transmissões e comunicações, com a internet da energia e a internet da logística que, ainda incipientes, fazem parte de uma infraestrutura inteligente integrada que passou a funcionar neste século e foi denominada de Internet das Coisas[1], gerando o aumento de produtividade ao ponto de o custo marginal de produtos e serviços serem quase nulos, sendo os mesmos praticamente gratuitos ou com custo marginal quase zero. As plataformas tecnológicas voltadas para o desenvolvimento da Internet das Coisas, conectarão mediante sensores e programas específicos, todas as coisas (máquinas, pessoas, recursos naturais, cadeias de produção , redes de logísticas, hábitos de consumo, fluxos de reciclagem e todo e qualquer aspecto da vida econômica), em uma rede mundial integrada (RIFKIN-2014,p.99).

[1] A expressão Internet das Coisas foi cunhada em 1995 por Kevin Ashon, um dos fundadores do Auto ID Center do MIT. E o fez em razão de o custo dos sensores e chips RFID de identificação por rádio frequência, que deveria incluir nas coisas era elevado. Posteriormente, estes custos das etiquetas eletrônicas foram se reduzindo até chegarem a dez centavos.

Quaisquer das duas possíveis revoluções citadas, funciona com base no conceito de Big Data onde plataformas de base tecnológicas gerarão a recepção e transmissão de quantidades maciças de dados que serão processados, analisados, e transformados por algoritmos preditivos que se programarão em um sistema automatizado que contribuirá para melhorar a eficiência termodinâmica das relações econômicas, com o consequente aumento da produtividade e redução quase a zero do custo marginal do produto ou do serviço.

A busca do crescimento sustentável e da lucratividade global como principal resultado esperado da utilização da IdC , nesta revolução em curso, será desenvolvida a partir da qualidade na interpretação de dados maciços e da aplicação em negócios e modelos econômicos, com as premissas decorrentes do sistema de regulação adotado no pais, no que tange a proteção de consumidores, dados, privacidade entre outros, que não desprezará direitos que corriqueiramente aparecem violados no uso diuturno e maciço da internet (SIMÃO FILHO,2015,p.37).

Como se observou, o Big Data como tratamento e análise maciça de dados de informações pessoais, pode redundar em efeitos positivos para os indivíduos e para a sociedade. Todavia, o direito de proteção de privacidade não pode ser rechaçado, pois possui natureza dúplice. Como direito autônomo protege algo valioso como a autodeterminação informativa, mas, ao mesmo tempo, sendo um direito instrumental, protege outros bens e interesses derivados, como a própria base digital de dados (SORO ET OLIVER-LALANA,2012, p.59).

O grande problema reside na busca da solução para o conjunto de efeitos negativos que podem ser gerados pelo sistema Big Data, no âmbito da invasão da privacidade e da intimidade e na tomada das decisões relacionadas à cadeia de consumo.

Este será o grande paradoxo e o Big problema que desafiará a legislação e os tribunais na busca da harmonização que possa evitar o sacrifício em demasia da privacidade.

3.A busca do direito à vida privada

Os historiadores não discordam de que os primeiros articulistas a tratarem do direito a vida privada foram Warren y Louis Brandeis (The Right to Privacy publicado em Harvard Law Review em 1890) que pretenderam solucionar um problema concreto consistente de analisar se o sistema *common Law* poderia dar respostas efetivas e concretas frente as intromissões à vida privada por parte dos órgãos de imprensa escrita e em face do uso de fotografias instantâneas publicadas.

Assim é que se construiu um embasamento teórico lastreado na tutela da propriedade privada, dignidade humana e inviolabilidade da personalidade, como forma de se justificar um sistema protetivo e o exercício de um certo controle sobre a vida privada, a ponto de garantir o direito de se decidir o que comunicar aos outros acerca dos seus pensamentos, sentimentos e emoções e em que nível.

Dentre os direitos da personalidade com tratamento e proteção constitucional e infra constitucional, situa-se o direito a vida privada, como previsto no Art. 5º, inciso X da Constituição Federal Brasileira de forma extensiva às pessoas jurídicas haja vista a ausência de definição do tipo de pessoa que poderia se utilizar desta proteção.

Do ponto de vista internacional, tanto a Declaração dos Direitos do Homem e do Cidadão de 1948 e demais ordenamentos da Comunidade Europeia como a Convenção Europeia dos Direitos do Homem de 1950, a proteção da vida privada faz parte de um conjunto de direitos essenciais para o ser humano, sendo a base para a conservação e a concretitude do principio da dignidade humana.

No âmbito da teoria dos círculos concêntricos relacionada à construção de critérios lógicos e objetivos para a valoração da privacidade (criada por Heinrich Hubman em 1953 e explicitada por Heinrich Henkel em 1957), onde na esfera maior se coloca a vida privada do cidadão, seguida pela esfera do meio situando a intimidade e confidencia e contendo no centro a esfera do segredo, a esfera da vida privada do individuo refere-se ao conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre as quais o interessado pretende manter controle exclusivo. Stefano Rodotá identifica esta privacidade como a "*tutela das escolhas de vida contra toda forma de controle publico e estigmatização social*" gerando a "*liberdade das escolhas existenciais" (RODOTÁ-1990).*

Observa-se que na esfera de vida privada há algum interesse público relacionado a certas circunstancias daquele cidadão, que são relevantes para a comunidade. Trata-se de acesso público especial e restritivo, todavia, plausível em face de interesses públicos. Na esfera da intimidade protegem-se relações intimas e não secretas, como o sigilo profissional, domiciliar e telefônico, gerando a necessidade de uma proteção mais ativa e afastando-se o acesso livre a certas informações. Já na esfera central e mais profunda, a proteção relaciona-se com segredos e opções sexuais, políticas, religiosas.

A definição de privacidade como o direito de estar ou de ser deixado só "*right to be alone*", deve também incorporar a nova definição contextualizada no direito de manter o controle sobre as próprias informações.

Estes direitos multifacetados que foram assegurados aos usuários pelo marco civil de internet, podem assim ser apresentados:

i) **Direitos Pessoais.** Inviolabilidade da intimidade, vida privada, sigilo no fluxo de comunicações pela internet ou comunicações privadas armazenadas (salvo por ordem judicial), sendo a garantia do direito à privacidade e a liberdade de expressão nas comunicações, condição para o pleno exercício do direito de acesso à internet.

ii) **Relativos a dados pessoais.** Salvo com o consentimento livre e expressamente exarado ou nas hipóteses legais, não podem ser fornecidos a terceiros os dados pessoais, registros de conexão e de acesso a aplicações de internet. As informações acerca da utilização dos dados pessoais, incluindo coleta, uso, armazenamento, tratamento e sistema protetivo devem ser claras. Os dados somente podem ser utilizados para finalidades que justifiquem sua coleta; não sejam vedadas pela legislação e estejam especificadas no contrato de serviços ou no termo de uso. Ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros na forma da lei, deve haver a exclusão definitiva dos dados pessoais fornecidos a determinada aplicação de internet.

A doutrina e as legislações consideram que o conceito de dado de caráter pessoal se subordina a possibilidade de se identificar de forma direta ou indireta as pessoas vinculadas à informação ou o seu sujeito ativo.

Ocorre que este conceito de dados pessoais pode restar insuficiente e inadequado observando-se as revoluções tecnológicas mencionadas anteriormente, quer a partir da utilização do Big Data em processamento de informações não estruturadas que possam também gerar reflexos em dados pessoais ou, ainda, a partir do advento da denominada Internet das Coisas conectando maquinas e pessoas ao limite.

Este fato, aliado a fragilidade da vinculação de usuário a determinados IP (*internet protocol*) fato que só enseja a identificação se o prestador de acesso de serviços em internet disponibilizar a informação faz com que inúmeros dados que se referem à intimidade de alguém e que podem ser considerados pessoais, resultem fora do alcance protetivo.

A questão se resume na necessidade de se ampliar o conceito relativo à descrição de dados pessoais para que se possa compor mais hipóteses protetivas alem das estudadas, para que não se caia na situação de ausência de cobertura e proteção legal, em casos onde não haja possibilidade de identificação do usuário (TORRIJOS,2013, p.46).

Neste ponto, como o sistema Big Data, opera na transformação de dados pessoais identificados e não identificados, estruturados ou não, para melhor compor perfil de consumidor, tornar-se-á necessário desenvolver linhas de pesquisa relacionando o direito do usuário de não ser molestado, mediante comunicações eletrônicas não solicitadas, visando oferta de produtos e serviços em momento imediatamente anterior àquele em que efetivou pesquisa sobre o tema na internet, por força da clara atuação Big Data no processamento de seus rastros digitais.

4.**(In)Vigilância liquida.**

Um dos elementos que contribuiu para a geração de uma aparente inércia na necessidade de proteção da vida privada na sociedade em rede contemporânea, talvez possa ser creditado à espetacularização da vida, gerando a falsa impressão de que se se tornar de alguma forma pública os fatos relacionados à intimidade do cidadão, este elemento por si, gerará melhores oportunidades no campo pessoal e profissional, com resultados positivos na sua vida.

Neste modelo, não se observa que nem toda a forma de comunicação ou trafego de dados deve ser pública, pois há que se preservar a dimensão da intimidade e da privacidade. Todavia, a convergência de mídia e a facilidade de interação faz com que o que era privado possa passar para esfera pública em questão de segundos, gerando uma exposição ampliada e replicada da pessoa, cujos resultados estão longe de serem avaliados (CODINA et OLLOQUI, 2014,p.29).

Alem destas situações deliberadamente colocadas, há ainda a submissão das pessoas a um nível de vigilância nunca visto ou sentido, que se liquefaz numa análise mais profunda dos seus elementos constitutivos.

Avalianso neste capítulo, a delicada e problemática questão dos dados maciços sob modelo Big Data, utilizou-se da consagrada expressão de Bauman sobre a vigilância que a todos submete sem permissão previa e sem limites claros, resultando num dilema de privacidade e dificultando o caráter protetivo e o alcance das regras disciplinatórias.

Esta vigilância se liquefaz, na nossa ótica, porque não se consegue ter claro quem nos vigia, porque nos vigiam, como nos vigiam e onde nos vigiam. Na realidade, a ausência de clareza destes princípios de vigilância, acaba por gerar uma não vigilância ou, ainda, como ousamos cunhar, uma invigilancia que pode ser proposital e lesiva aos interesses coletivos de pessoas que não dispõem de ferramentas que possam fazer exercitar plenamente o seu controle, proteção e tutela do direito a vida privada e dignidade.

Talvez uma parte da vigilância sofrida, venha dos próprios poderes públicos como forma de exercitar o governo e gerar segurança. A limitação de direitos de base constitucionais em face da segurança, onde se inclui os que se relacionam a vida privada, não é desconhecida e é aceita legitimamente em muitas partes.

Observa-se a exemplo, que o direito ao respeito à vida privada estabelecido pela convenção Europeia de Direitos Humanos, quando na visão jurisprudencial do Tribunal Europeu de Direitos Humanos, sofreu condicionantes com a formulação dos estritos requisitos que se deve cumprir quando se necessitar interferir na vida privada e no tratamento de dados sobre pessoas.

Assim é que as legislações da União Europeia passaram a prever exceções e limitações ao nível de proteção das pessoas, com relação ao tratamento de dados pessoais estabelecidos, em nome da segurança (FUSTER, 2014,p.68).

Mas, será mesmo que, enquanto cidadão, para se ter uma melhor proteção governamental e segurança, se tem que ceder espaço e abdicar da plenitude de direitos constitucionais legitimamente conquistados, relacionados à privacidade, intimidade e dignidade?

Neste ponto assevera Victor Domingo Prieto para que os Estados possam cumprir interesses jurídicos legítimos e, preponderantes e importantes no âmbito de uma sociedade democrática e, ainda, efetivamente as suas obrigações decorrentes de legislações internas e internacionais sobre os direitos humanos em contraposição à vigilância exercida nas comunicações, devem respeitar certos princípios onde a segurança nacional está incita, obrigando-se a respeitar e garantir os direitos individuais assim como tendo o dever de proteger os direitos das pessoas em face da potencialidade de a vigilância acabar por revelar informações protegidas ou de abusos praticados por atores não estatais (PRIETO,2014 ,p.38).

Pesquisas recentemente efetuadas na Espanha acerca do tema do conflito entre a privacidade e a segurança pública, onde se apresentou às pessoas situações de conflitos especialmente polêmicos e atuais como os relacionados às atividades policiais e luta contra o terrorismo, redundando na necessidade de vigilância acirrada nas comunicações privadas, demonstraram que a maioria dos entrevistados foi favorável a proteção da segurança publica e fiscalização das comunicações privadas, relegando ao segundo plano a proteção à privacidade e intimidade. Observa-se que esta mesma pesquisa quando realizada no ano de 2006 gerou uma adesão de 44,81% de pessoas favoráveis e repetida em 2009, gerou a concordância de 50,56% demonstrando a contraposição por parte destas pessoas, a uma cultura política com relação ao tratamento de dados pessoais em momentos de tensão social, quando se está a frente de sistemas individuais protetivos como o relacionado à privacidade e intimidade (SORO et OLIVER-LALANA,2012,p.128).

A outro lado, a grande revolução no progresso da sociedade consumista ocorrida de alguns anos a esta parte, segundo Bauman, se dá na passagem da satisfação das necessidades através de produção lastreada na demanda existente, para a criação de necessidades por meio de tentação, sedução e estímulo do desejo despertado pelo produto ou serviço, gerando uma nova demanda voltada exatamente para a produção já existente (BAUMAN,2013,p.116).

A partir das revoluções geradas pela utilização do Big Data e com o advento da Internet das Coisas - IdC, multiplicam-se os meios de controle e de vigilância refletindo na geração de dados estruturados e não estruturados.

Desta feita, a vigilância praticamente se dá em todos os ambientes que o cidadão frequenta. Locais públicos e privados de qualquer natureza, possuem câmeras que registram movimentos e, em muitos casos, o som do ambiente. Redes sociais usam de meios tecnológicos para processar e transmitir na velocidade do pensamento, o conjunto de dados sequenciais, decorrentes da transformação tecnológica de sons, diálogos, fotografias, vídeos, possibilitando, através de seus geolocalizadores tecnológicos, determinar com margem de segurança e precisão, os locais de onde são provenientes as transmissões e, por via de consequência, detectar onde se encontra a pessoa, numa aparente ou clara invasão de privacidade.

A vigilância constante aliada ao tráfego intenso de dados que são analisados e monetizados, gera como consequência primária, a detecção de padrão de consumo e o assedio sobre consumidores em potencial, que acabam por sofrer manipulação com a geração de falsas necessidades criadas por meio de ofertas

O processo de reestruturação do capitalismo, com sua lógica mais rigorosa de competitividade econômica, segundo Manuel Castells, seria o responsável por boa parte do sofrimento imposto ao refletir sobre as desigualdades sociais que ocorreram com o surgimento do informacionalismo (CASTELLS,2012,p.95).

As novas condições tecnológicas e organizacionais próprias da Era da informação, provocam uma reviravolta no velho modelo do lucro que passa a deter outras variáveis imateriais na sua construção plena, decorrentes da utilização de plataformas tecnológicas nos negócios e nas relações humanas.

Uma economia, sociedade e cultura construídas com base em interesses, valores, instituições e sistemas de representação que, em termos gerais, limitam a criatividade coletiva, confiscam a colheita da tecnologia da informação e desviam a energia para o confronto autodestrutivo (CASTELLS,2012,p.437), não deve ser vista como um bom resultante destas tecnologias que compõe estas propaladas revoluções industriais, lastreadas na garimpagem de dados como se fossem as novas pepitas ou pedras preciosas da sociedade informacional e na utilização da Internet das Coisas como se não houvesse um amanha ou um passado de construção da proteção dos direitos individuais e das garantias nos países.

O estado de vigilância constante e a necessidade de proteção de dados pessoais gera uma dilema e, segundo Rodotá, uma abordagem marcadamente contraditória tanto na proteção dos dados pessoais como nas questões correlatas inerentes e uma verdadeira esquizofrenia social, política e institucional (RODOTÁ,2008,p.13).

Outro aspecto bem demonstrado por Bauman, refere-se a vigilância constante e intermitente da pessoa e ao processamento e canalização de dados sensíveis pessoais, como fatores que podem contribuir para a construção de perfis de minorias indesejáveis, gerando a potencialidade de exclusão social ou de normalização de grupos não excluídos que passariam a ter melhores condições de acessos aos bens corpóreos ou incorpóreos de consumo (BAUMAN,2013,p.65).

Neste ponto, a operação de Big Data analisando maciçamente os dados gerados pelos dispositivos de estrita vigilância, acaba por se prestar a ser instrumento de uma política no modelo *Surveillance State,* para identificar prontamente indivíduos que deem sinais de não estarem dispostos a se manter na linha socialmente desejável ou, ainda, que planejem quebrar paradigmas obrigatórios.

E não parece que esta interação internet, vigilância e máquinas será algo que conterá a utilização do Big Data ou gerará um regramento eficiente. Segundo Rifikin, a IdC será a primeira revolução da história baseada em uma infraestrutura inteligente que conectará cada máquina, cada empresa, cada veículo a uma rede inteligente formada por uma internet das comunicações, uma internet da energia e uma internet da logística integrada em um único sistema operativo (RIFKINS,2014 ,p.97). A conexão de pessoas e todas as coisas em uma imensa neuro rede mundial como proposta pela IdC, é apaixonante e desafiadora, abrindo na visão de Rifkins, na coexistência na terra, uma possibilidade que apenas se pode vislumbrar no início desta nova era da historia humana (RIFKINS,2014 ,p.103). O desafio será equilibrar as necessidade dos agentes que operam a IdC com os direitos que se pretende sejam protegidos.

5.As premissas de um Sistema protetivo eficiente de base de dados, a partir do ordenamento brasileiro e europeu e a crise do modelo.

As leis de proteção dados pessoais, consagram o regime de tutela das liberdades contra os perigos e ameaças à privacidade do tratamento digital ou não, do conteúdo de bancos de dados e especificamente o art.43 do Código de Defesa do Consumidor brasileiro, disciplina a necessidade de gerar ao usuário o acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes (KLEE et MARTINS,2015,p.325).

Ainda, observando-se o direito do consumidor brasileiro, para que um tratamento de dados pessoais possa ser legitimamente efetuado, considera-se como regra geral que o mesmo tenha sido autorizado pelo consumidor titular dos dados, salvo excepcionalidades legais, considerando-se também critérios como boa fé objetiva, expectativas legitimas do consumidor, impactos e riscos gerados pelo tratamento de dados para o consumidor (MENDES,2015,p.478).

A Lei n. 12.965/2014 conhecida como o marco civil da internet prevê o direito de acesso à internet como essencial ao exercício da cidadania; a proteção da privacidade como regra de principio; a proteção aos dados pessoais, a inviolabilidade da intimidade e da vida privada, a inviolabilidade e sigilo do fluxo de comunicações em internet, inviolabilidade e sigilo das comunicações privadas armazenadas e, ainda, a garantia do direito à privacidade e à liberdade de expressão como condição para o pleno exercício do direito de acesso à internet. (vide artigos 3º III;art.7º incisos III,VII e IX e Art.8º)

Como aponta Cintia Lima o legislador brasileiro acabou por adotar o principio da autodeterminação informacional fundado na perspectiva de que o próprio usuário deve ter controle sobre as suas informações pessoais autodeterminando-as, gerando a necessidade de se exigir o consentimento do titular dos dados pessoais para que os mesmos possam ser coletados, processados, compartilhados. Este modelo é replicado tanto na edição dos guidelines da Organisation for Economic Co-operation and development/OECD em 1980 como nas legislações do Canada, Argentina e União Europeia (LIMA et BIONI,2015,p.267).

Os estudos norte americanos sobre o tema caminham para um conceito conhecido como *privacy by default* como forma de se melhorar e gerar eficiência ao principio da autodeterminação e do consentimento informado. Trata-se do uso da tecnologia para que se possa configurar o padrão dos navegadores de forma tal que a proteção de dados pessoais se faça a partir da coleta destes dados gerando uma corregulação implementada por uma simbiose entre direito e tecnologia na busca de melhor proteção da privacidade (LIMA et BIONI,2015,p.277).

A análise do acesso à base de dados possui uma dimensão negativa que consiste na existência de uma esfera de interesses pessoais que deve estar isenta de acesso de terceiros e outra positiva onde o titular dos dados possui o controle a respeito de acessos, retificações de dados, inclusões, supressões, impugnações e divulgações, gerando a possibilidade restritiva e protetiva.

Como visto, legislações, doutrina e jurisprudência de vários países como os da Europa Comunitária, acabaram por adotar um direito fundamental à autodeterminação informativa baseado no direito geral da personalidade que oferece proteção alguns princípios gerais que se tornaram cerne do sistema protetivo de base de dados e dados pessoais.Os principais princípios são (ROTONDO,2015,p.33):

i) **Legalidade:** A base de dados devem ser registradas e não pode ter finalidade que viole direitos humanos ou que seja contrárias as leis e a moral.
ii) **Veracidade:** Os dados pessoais que sofrem tratamentos em base de dados, devem ter veracidade, adequação e equanimidade, sem excessos com relação à finalidade pela qual tenham sido obtidos, sendo passíveis de correção ou cancelamento.
iii) **Finalidade:** Os dados não podem ser utilizados para finalidades diferentes ou incompatíveis com aquelas que motivaram a sua obtenção e devem ser suprimidos quando tenham sido deixado de ser necessários ou pertinentes aos fins pelos quais foram coletados.

iv) **Segurança**: Os responsáveis ou usuários de uma base de dados pessoais devem adotar medidas eficientes para protegê-la contra adulterações, perdas, destruição ou acesso não autorizado.Deve-se proibir o registro de dados pessoais em bases que não reúnam as condições técnicas de integridade e segurança.

v) **Reserva:** O uso da base de dados deve ser exclusivo para operações habituais do responsável pela base, devendo ser assegurada a confidencialidade dos dados pessoais, com proibição de difusão a terceiros.

vi) **Responsabilidade por violações normativas**.

vii) **Prévio consentimento informado.** Torna-se ilícito um tratamento de dados pessoais sem consentimento. O consentimento deve ser livre, prévio, expresso e informado. Caso os dados tenham origem em fontes públicas, o consentimento não é necessário.

No contexto europeu e particularmente na Espanha, na análise de casos específicos, se efetua a distinção entre a privacidade, direito à intimidade e direito a proteção de dados. A título de ilustração, o direito a autodeterminação informativa nasce na República Federal da Alemanha com a sentença proferida em 1983 pelo Tribunal Constitucional Federal Alemão (TCFA) sobre a Lei do Censo que foi considerada parcialmente inconstitucional. Afirmou-se nesta oportunidade que o direito geral de personalidade comporta a atribuição ao indivíduo da capacidade de decidir no exercício de sua autodeterminação, que extremos deseja revelar de sua própria vida. Esta autodeterminação pressupõe também nas condições das técnicas modernas de tratamento da informação, que se conceda ao individuo a liberdade de decisão sobre as ações que realizará ou, ainda, de omissão onde se inclui a possibilidade de agir de fato na forma que seja sintonizada com a decisão que adotou.

Esta liberdade de decisão e de controle pressupõe que o individuo tenha o direito de acesso aos seus dados pessoais, tendo conhecimento do que se processa sobre sua pessoa como também de submeter o uso destes dados a um controle por autodeterminação tanto do armazenamento destes dados pessoais como de sua utilização e transmissão. O direito fundamental de proteção de dados é assim um direito de natureza prestacional onde se possibilita a pronta reação em face da vulneração como também a tutela judicial e administrativa visando a retificação ou cancelamento dos dados e gerando deveres e obrigações aos responsáveis (MARTINEZ,2014,p.54).

Enquanto nos EUA se opera princípios de livre comercio e *opting out*, na proteção dos dados, na União Europeia se reforça a metodologia do consentimento expresso e a posição jurídica da pessoa afetada, prestigiando-se os direitos fundamentais e criando instrumentos de apoio na proteção como a figura do Data Protection Officer como uma entidade protetora de dados a exemplo da Agencia Española de Protección de Datos (AEPD)

A apropriação pelo particular, de dados pessoais e sensíveis, representa na atualidade, como menciona Podesta, um valor econômico que viabiliza a manipulação do comportamento social e a defesa da privacidade e da dignidade como um componente essencial da pessoa humana e uma condição para a igualdade e liberdade. (PODESTA, 2015,p.389)

A questão problematizada neste artigo, acerca das revoluções tecnológicas ultimas que redundaram na utilização da internet de maneira ampla e absoluta, com tratamento de dados de forma maciça, acaba por contribuir para a conclusão de que o modelo individualista proposto para a proteção da privacidade e da intimidade sob regime de autodeterminação, já não mais atende às expectativas protetivas, encontrando-se em franca crise.

As práticas de análise maciça de dados acabam por banalizar a ideia do tratamento consentido de dados. Já há doutrinadores que defendem não só a visão do consentimento como um mito em face justamente das experiências com dados maciços tratados indiscriminadamente, como também que já apregoam a crise do modelo individualista de proteção de dados que não consegue atender a abrangência da noção de controle e uso da informação e a ambivalência do consentimento.

Tanto a utilização de Big Data como a implantação da inteligência artificial que possibilita gerar decisões automatizadas ou influir na tomada de decisões, fere a lógica do consentimento informado e redunda na criação de base de dados cujo caráter protetivo de privacidade é questionável, levando-se à consequência de se supor a necessidade de migração do modelo individualista de autodeterminação para um modelo que possa abranger a importância da privacidade como um bem social e a partir de então, gerar uma tutela mais ampla e eficiente (OLIVER- LANANA et SORO, p.155).

Enquanto não se legisla sobre os aspectos relacionados ao tratamento maciço de dados e suas consequências na tutela da privacidade, concordamos com Danilo Doneda quando ao analisar os princípios protetivos dos dados pessoais, acaba por constatar que tais princípios revelam muito mais do que demandas setoriais, valores gerais ou até a vinculação com a funcionalização de uma garantia fundamental de proteção dos dados pessoais. Por esta razão, mais do que serem considerados dentro do espectro de sua normativa, devem os mesmos ser interpretados de forma extensiva para considerar abarcar e proteger todas as situações nas quais possam propiciar a tutela concernente com as características da atual sociedade tecnológica informacional (DONEDA,215,p.384).

Aspectos conclusivos

A pesquisa demonstrou que a tutela legal e de proteção de dados pessoais se faz atendendo ao principio da autodeterminação presente tanto no marco civil de internet, Lei 12.965/14 como nas legislações estrangeiras. As base protetivas operam para gerar tutela ao direito pessoal de inviolabilidade da intimidade, vida privada, sigilo no fluxo de comunicações pela internet ou comunicações privadas armazenadas aliado à garantia do direito à privacidade e a liberdade de expressão nas comunicações.

Observada a dinâmica da internet em ambiente de Sociedade da informação e as constantes inovações tecnologicas, foram verificadas empiricamente, duas revoluções digitais que basicamente trabalham com referenciais assemelhados.

A primeira refere-se á revolução dos negócios baseados em dados onde um conjunto de dados inseridos em base digital, passa a atingir valor econômico inimaginável, a depender de sua forma de organização, conteúdo e arquitetura tecnológica de acesso, sofrendo intensa monetização. O sistema de processamento destes dados e informações que trafegam em internet, onde se incluem dados sensíveis, públicos, sigilosos ou de qualquer outra natureza, por meio de ferramentas tecnológicas no modelo Big Data acaba por gerar o tratamento e seleção de um volume maciço destes dados, que são utilizados em áreas das mais diversas, gerando um mundo onde a característica maior é a otimização ao infinito do processo de captação e prospecção de clientela e de vigilância continua em desprestígio à privacidade e intimidade do usuário.

A segunda revolução analisada, refere-se a utilização de uma plataforma de base tecnológica sob o conceito de Internet das Coisas-IdC, que opera tanto nas transmissões e comunicações de dados, como na energia e logística, através de uma infraestrutura inteligente integrada que conectará, mediante sensores e programas específicos, máquinas, pessoas, recursos naturais, cadeias de produção, redes de logísticas, hábitos de consumo, fluxos de reciclagem e todo e qualquer aspecto da vida econômica, gerando o aumento de produtividade e redução de custo marginal de produtos e serviços a ponto de estes serem quase reduzidos a zero em uma rede mundial integrada.

Neste ambiente informacional e tecnológico, a análise permitiu demonstrar que apesar do avanço legislativos da legislação brasileira e do ordenamento europeu acerca da proteção de dados pessoais, não há ainda uma harmonização dos interesses pessoais e econômicos gerados pelo sistema Big Data, que possa levar a completa proteção da privacidade ou, ainda, à eficiência do sistema de autodeterminação. Neste ponto, o estado de vigilância liquida e constante, exercido contra todos, por meio tecnológico, aliado a necessidade de se gerar a efetiva proteção e segurança de dados e a segurança das pessoas, acaba por confirmar o paradigma de conflito, cuja solução não é possível ser feita no estrito âmbito desta pesquisa, por necessitar de melhor desenvolvimento teórico e doutrinário que considere exatamente a evolução tecnológica.

A crise do modelo protetivo de autodeterminação, a partir do qual a proteção dos dados pessoais se dá parte do fato demonstrado de que muitos dos dados pessoais trafegados por internet ou prospectados por meio de geolocalizadores, selecionados e transformados por procedimentos de Big Data, sequer são de conhecimento do usuário, não tendo o mesmo, portanto, a condição de interagir na sua proteção ou na busca de tutela preventiva.

Enquanto não se elaborem regras mais específicas para abranger os efeitos das revoluções tecnológicas citadas, com relação à tutela da privacidade, talvez o caminho factível para uma das soluções ao problema inicialmente posto, seja ampliar a percepção do que se entende por dados pessoais e da condição de aplicabilidade e de interpretação extensiva das regras atuais, para que se possa minimamente contemplar também a proteção o cidadão em face do uso abusivo de dados pessoais e informações maciçamente processadas e obtidas que acabam por gerar uma nova cadeia de valor formada às custas da invasão da privacidade e da intimidade alheia.

Referencias bibliográficas.

Alejandre,Gemma Minero. La protección jurídica de lãs bases de datos em El ordenamiento europeo, Madrid: Editorial Tecnos. 2014.

Bauman,Zygmunt. Vigilancia Líquida.Diálogos com David Lyon, Rio de Janeiro: Zahar,2013.

Capitán,Eva R.Jordà ET Fernández,Verónica de Priego. La protección y seguridade de La persona em internet.Aspectos sociales y jurídicos, Madrid:Editorial Reus.2014.

Castells,Manuel. Fim de milênio. A era da informação: economia, sociedade e cultura, São Paulo: Paz e Terra, Vol 3.2012.

--- A Sociedade em rede.A era da informação:economia, sociedade e cultura, São Paulo: Paz e Terra, 6ª Ed.Vol 1, 2010.

Codina,Mónica ET Olloqui,Isabel.Quién controla AL controlador? Entender La comunicación em La nueva aldea global,Navarra:Ediciones U.de Navarra. 2014

Doneda,Danilo.Principios da proteção de dados pessoais, p.369 a 384, In Direito e Internet III, org.Adalberto Simão Filho, Newton De Lucca e Cintia R.P.Lima, São Paulo:Quartier Latin, 2015.

Fuster,Glória Gonzales. La privacidad em Europa Um debate cada vez más fundamental o cada vez menos? Revista Telos, Pensamewnto sobre comunicacíon,tecnologia y sociedad97, p.64 a 72,Madrid:Fundação Telefonica,fever/maio,2014.

Giménez,Alfonso Ortega ET Martínez,José Antonio González. Buenas prácticas para entidades financeiras em material de protección de datos de carácter personal,Madrid:Difusión Jurídica.2010.

Jiménez,David López ET Dittmar,Eduardo Carlos. Internet móvil y geolocalización:nuevos retos para La privacidad em La era digital, p.519 a 542, in La proteccíon de lós datos personales em internet ante La innovacíon tecnológica, Org. Julián Valer oTorrijos,Navarra:Ed.Aranzadi,2013.

Klee,Antonia Espindola Langoni ET Martins, Guilherme Magalhães. A privacidade, a proteção dos dados e dos registros pessoais e a liberdade de expressão:algumas reflexões sobre o marco civil da internet no Brasil. (p.291 a 367), in Direito e Internet III, org.Adalberto Simão Filho, Newton De Lucca e Cintia R.P.Lima, São Paulo:Quartier Latin, 2015.

Lima,Cintia Rosa Pereira et Bioni,Bruno Ricardo. A proteção dos dados pessoais na fase de coleta: apontamentos sobre a adjetivação do consentimento implementada pelo art. 7, incisos VIII e IX, do Marco Civil da Internet a partir da Human Computer Interaction e da privacy by

default,(p.263 a 287), in Direito e Internet III, org.Adalberto Simão Filho, Newton De Lucca e Cintia R.P.Lima, São Paulo:Quartier Latin, 2015.

Martinez,Ricard. Privacidad,Estados Unidos y España.Tan lejos,tan cerca.In Telos 97.Revista de pensamento sobre comunicação,tecnologia e sociedade, p.48 a 56,Madrid:Fundação Telefonica.Fevereiro-mayo-, 2014.

Mayer-Schönberger,Victor et Cukier, Kenneth. Big Data- La revolución de los datos masivos, Madrid:Turner Publicaciones, 2013.

Mendes, Laura Schertel. A Tutela da privacidade do consumidor na internet: Uma análise à luz do marco civil da internet e do código de defesa do consumido, p.471 a 501, in Direito e Internet III, org.Adalberto Simão Filho, Newton De Lucca e Cintia R.P.Lima, São Paulo:Quartier Latin, 2015.

Mirete.Carmen Maria Garcia. Las bases de datos electrónicas internacionales,Valencia:Tirant lo Blanch.2014.

Oliver-Lanana,A.Daniel et Soro,José Felix Muñoz. El mito del consentimiento y el fracasso del modelo individualista de protección de datos,p.153 a 196,in La protección de los dadtos personales en internet ante la innovación tecnológica, Org. Julián Valero Torrijos, Navarra:Ed.Aranzadi,2013.

Prieto,Vitor Domingo.De la defensa del derecho fundamental a la privacidad a la vigilancia masiva.In la protección y seguridad de la persona en internet.Aspectos sociales y jurídicos, p.35 a 47, org. Eva R.Jordá Capitán et Verónica de Priego Fernández,Madrid:Editorial Reus,2014 .

Podesta,Fabio Henrique, Marco Civil da Internet e direitos da personalidade, p.385 a 403, In Direito e Internet III, org.Adalberto Simão Filho, Newton De Lucca e Cintia R.P.Lima,São Paulo:Quartier Latin, 2015.

Rifkin,Jeremy. La sociedad de coste marginal cero. El internet de las cosas El procomum colaborativo y el eclipse del capitalismo, Barcelona: Paidós,1ª Ed.,2014.

Rodotá,Stefano. A vida na sociedade da vigilância. A privacidade hoje, Rio de Janeiro: Renovar,2008.

Rotondo, Felipe. Acesso a La información pública y protección de datos personales:Conceptos y su aplicación,p.31 a 48, in Direito e novas tecnologias da informação.Org Rafael Santos de Oliveira, Curitiba:Ithala,2015.

Salom, Javier Aparicio. Estudio sobre La protección de datos, Navarra:Thomson Reuters,2013.

Schmarzo,Bill. Big data, El poder de los datos, Madrid:Anaya. 2013.

Simão Filho,Adalberto. Revisitando a nova empresarialidade a partir do marco civil em contexto de internet das coisas,p.27 a 47, in Direito e Internet III, org.Adalberto Simão Filho, Newton De Lucca e Cintia R.P.Lima. São Paulo:Quartier Latin, 2015.

Soro,José Felix Muñoz ET Oliver-Lalana.A.Daniel. Derecho y cultura de proteccion de datos, Um estúdio sobre La privacidad em Aragón, Madrid: Dykinson,S.L. 2012.

Torrijos,Julián Valero. La protección de lós datos personales em internet ante La innovación tecnológica. Riesgos, amenazas y respuestas desde La perspectiva jurídica, Navarra:Thomson Reuters, 2013.